European Organization for Nuclear Research (CERN)

Dr. Christos Zamantzas
Beams Department (BE)
CH - 1211 Geneva 23
Switzerland

Tel: +41 22 767 3409
Mob: +41 76 487 2170
email: christos.zamantzas@cern.ch

External Review of the CERN LHC Beam Loss Monitoring System

30th June 2010

Motivation for an External Review:

In order to ensure the safety of LHC in the presence of circulating beam it is expected that the Beam Loss Monitoring System functions correctly. It is clear that a failure of this system to detect particle flux above the specified limits and issue in the required time period the emergency beam dump request has the potential to cause substantial damage to the LHC accelerator and its experiments, risking the future of the LHC and the organisation.

Amongst other things, BE/BI/BL has a large responsibility for the design and realisation of this system. All possible steps to our knowledge have been and should be taken to ensure that the Beam Loss Monitoring System is of the highest quality, suitable for protecting the LHC.

With this in mind, an internal review of the Beam Loss Monitoring System was carried out in 2008, which showed the system to be of a high-standard, and compliant with the requirements of safety and availability. During this review some 46 action points were raised which have been progressively addressed over the course of the last two years.

Since then, several requirements have been augmented, mostly based on the experience gained during the commissioning period, and several adjustment have been enforced in order to suit and provide better integration into CERN infrastructure and daily operation.

Following from this, 2010, the moment where LHC commissioning phase ends and beams with higher damage potential are foreseen, presents a valid and viable opportunity to carry out an external review of the LHC Beam Loss Monitoring System, to further assess and enhance the studies made concerning the risk of the Beam Loss Monitoring System failure.

In specific:

1. **The 2008 internal review used only accelerator professionals.**
   It would be more appropriate, given the nature of the system, to use a dedicated safety company to carry out this work. Involving experts who work in the public and private sectors, on systems which have certified safety, which perform similar tasks as those the BLMS is doing.

2. **During the 2008 internal review several parts of the reprogrammable components had not yet been completed or have changed significantly since.**
   It would be more appropriate, given the nature of the system, to repeat the review at this point in time where all request and changes have been fulfilled and the code has been accepted as stable by the designers.
   In addition, involving experts who are independent from the Machine Protection System infrastructure will assist identifying errors common across the different systems employed.
3. **There is no means of referencing the Beam Loss Monitoring System design to other monitoring and measurement systems in industry**
   An external review can compare the implementation of the Beam Loss Monitoring System to that of other systems used in public and private sector.
4. **VHDL (software/firmware) safety is difficult to quantify.**
   The Beam Loss Monitoring System relies substantially on the implementation of VHDL. Whilst every effort has been made to create a robust code, it is not clear whether our methods match those made by other individuals in private industry.
5. **CERN has other systems which would benefit from generic review methods**
   In using an external company who has dealt with many such reviews as this, it will be possible for CERN to take a generic 'review methodology' from the work to use in future internal and external reviews.
   Moreover, BE/BI/BL is requested during the renovation of all CERN injectors to facilitate them with similar protection systems. Acquiring advance knowledge on the subject will provide better results and reduce costs.
6. **Comparison of the system to international standards, such as DO-178B**
   BE/BI/BL currently does not have the expertise to certify a system, or design a system to a safety standard, using an external company which has expertise in these domains will give CERN an indication of whether there is a big difference between the in-house techniques developed, and those required for a full certification.

Choice of Company:

The choice of the company used for the external review is critical to achieve the goals set for such a review. BE/BI/BL has considered several candidate companies which were known internally to CERN:

HYTEC & SCOTLAND ELECTRONICS INTERNATIONAL LTD
Both Hytec Electronics and Scotland Electronics International are service providers who specialise in turn-key solutions for industrial control applications. These initially appear as good choices for an external review of the Beam Loss Monitoring System. However, their primary focus is on system design and realisation, not reviewing for safety. CERN needs a company who is an expert in system study and review, who has a vast experience in safety systems, a wide knowledge of safety standards and deep experience in nuclear, military, and aerospace safety – these are the only industries similar to CERN in this respect. The Beam Loss Monitoring System audit in 2008 already covered the aspects of the design which both Hytec and Scotland Electronic could cover as external reviewers.

DOULOS LTD
Doulos provide training and experience in VHDL and other Hardware Description Languages. Doulos taught an Expert VHDL Verification course at CERN which formed the basis of the design rules for parts of the system; therefore this company is well suited to the task of code auditing. However, they have no advertised experience in any other area related to electronics verification (outside of the HDL domain), thus they are not suited to a broad review of the Beam Loss Monitoring System such as required.

INTECSA UHDE INDUSTRIAL S.A. and SCHNEIDER ELECTRIC
Both Intecsa and Schneider provide turn-key plant and Engineering-Procurement-Construction, they are not experienced in high-risk safety systems, such as nuclear, military, or aerospace safety systems.

INTRACOMDEFENSE
One promising candidate is Intracomdefense who were approached by the Beam Dump System experts to carry out an external review of the Trigger Synchronisation Unit. This company looked the closest candidate to carry out a similar review of the Beam Loss Monitoring System. However, following a period of initial study, the company declined to make an offer to CERN for the services of an external review for the Beam Dump System; it is therefore unlikely that a similar review of the Beam Loss Monitoring System would be accepted by the company.

CRITICAL SYSTEMS LABS INC.
In 2008, CERN attended the 26th International System Safety Conference, chaired by Dr. Jeff Joyce of Critical Systems Laboratories Inc (**CSL**).

http://www.cslabs.com/

Critical Systems Labs have highly specialised knowledge of the relationship between software functionality and safety risk in many different domains, these match CERN's review requirements.

One of the key elements of such a review is the role VHDL (software/firmware) plays in the protection of CERN accelerator complex, and whether a system is suitably designed to minimise the risks this poses. This area, software/firmware in critical applications, is a strength of CSL.

CSL had have an in depth review of the Beam Interlock System (BIS) in 2009. The Beam Loss Monitoring System has a strong dependency in the BIS expecting from it to correctly receive and propagate its beam dump request as well as to inform on the beam status.

- **CSL is accustomed with the CERN infrastructure.**
- **CSL has advance knowledge on the inner workings of the systems that the Beam Loss Monitoring System depends to propagate its information.**
- **CSL has advance understanding of the expectations by the systems the Beam Loss Monitoring System depends and could identify wrong assumptions by the different designers between systems and incompatibilities introduced.**

In addition, CERN should also consider implementing a safety standard (such as DO-178B, MIL-STD-882, IEC-61805) to qualify the whole Machine Protection System. BE/BI/BL could participate in such an effort, and understanding just how far current systems are from compliance is a big requirement.

- **CSL have an up-to-date experience in DO-178B**
- **Members of RTCA SC 205, CSL contribute to the development of DO-178C**
- **CSL have an up-to-date experience in multiple defence standards including MIL-STD-882**
- **CSL have experience in IEC-61508**

CERN has invested in test equipment to ensure the correct performance of systems, these test systems should be considered for their impact on safety

- **CSL has experience in testing safety-critical applications and real-time systems**

Mr. M. Kwiatkowski is currently studying a PhD at CERN in 'VHDL for safety systems' amongst his research is the topic of formal methods for the complete mathematical verification of the correct functionality of a software system. CERN should know whether the VHDL used in the Beam Loss Monitoring System can be subject to formal methods.

- **CSL have experience in formal methods**

As no such comparable machine to LHC exists anywhere else in the world, it is best to choose a company who has a wide experience in a wide range of safety domains:

- **CSL has collaborated with university and industry partners to develop new methods for detecting potential sources of safety risk in advanced software-intensive electronics controls for road vehicles**
- **CSL is also an active participant in ISO TC22/SC3/WG16, an international working group developing a new international standard for the functional safety of electronic controls systems in road vehicles.**
- **Dr. Jeffrey Joyce of CSL has contributed to draft versions of this (proposed) standard with input on a variety of subjects, as Canada's designated technical expert for this working group.**
- **CSL consultants have worked on operational control systems and simulators for air traffic management in North America, Asia Pacific and Europe.**
- **CSL has experience in Radar Data processing, Flight Data Management, Safety-net tools such as Conflict Prediction and Minimum Safe Altitude Warnings.**

CERN has had to keep the cost of the Beam Loss Monitoring System down, and has had to make a system which is both very safe and very available. To do this CERN has had in many cases to take advantage of the Commercial off the Shelf (COTS) components, which provide a cost-effective solution, but can pose questions over safety.

CERN also needs to develop in a more general way to integrate safety into more systems. CSL have proven experience in similar situations.

- **CSL can introduce / enhance the safety process within systems / software engineering organization**
- **CSL will help us developing and establishing a Safety Culture**
- **CSL will help us develop safety assessment guidelines**

To be effective, this review must take place before the end of September, to allow conclusions to be implemented in the system before LHC commences further in high-intensity operation.

- **CSL can come to CERN the second week of September.**

In Summary

BE/BI/BL has been asked to carry out a full review of the Beam Loss Monitoring System before LHC enters in high intensity operation. For this review to be effective it must be carried out before the middle of September, thus any limitations which are identified in the system can be quantified and addressed in time. BE/BI/BL fully acknowledges that Member State companies may be able to carryout the requirements of the review, but only after a detailed vetting, and market survey.

It is the conclusion of BE/BI/BL that the external review of the Beam Loss Monitoring System can only be carried out to the required standard within this short time-scale by Critical Systems Labs. Inc.

Alternative solutions involving a market survey, vetting, and tendering are possible, but would delay the review until after unprecedented beam intensities are foreseen in LHC, which is not acceptable.

In addition, CSL are completely independent from the accelerator community, having considerable experience in the domains which are closest to that which is represented by the LHC and Machine Protection.

CSL has reviewed the Beam Interlock System in 2009 and therefore holds significant understanding of the surrounding infrastructure, has gained in depth knowledge of the LHC machine in respect to the specifics of the review requested and has proven its diligence and advance knowledge in the subject.

A comparison of the Beam Loss Monitoring System with other industry standards will be highly beneficial. Moreover, CERN must be categorically sure of the LHC Machine Protection System dependability before the machine enters further in the unsafe regime.

One must also consider that the proposed cost is orders of magnitude lower than the cost of repairing potential damage which would be incurred given a blind failure of the Beam Loss Monitoring System. It must be noted that the Beam Loss Monitoring System is **the only way** to detect and request an emergency beam dump from beam losses that deposit enough energy on those elements to be destructive in a time period below 10 ms.

This review with CSL as reviewers will give CERN the confidence to operate the LHC machine, knowing it is equipped with a state of the art Machine Protection System, designed to protect CERN's investment, and the future of High Energy Physics in Europe.